protiviti®

Face the Future with Confidence

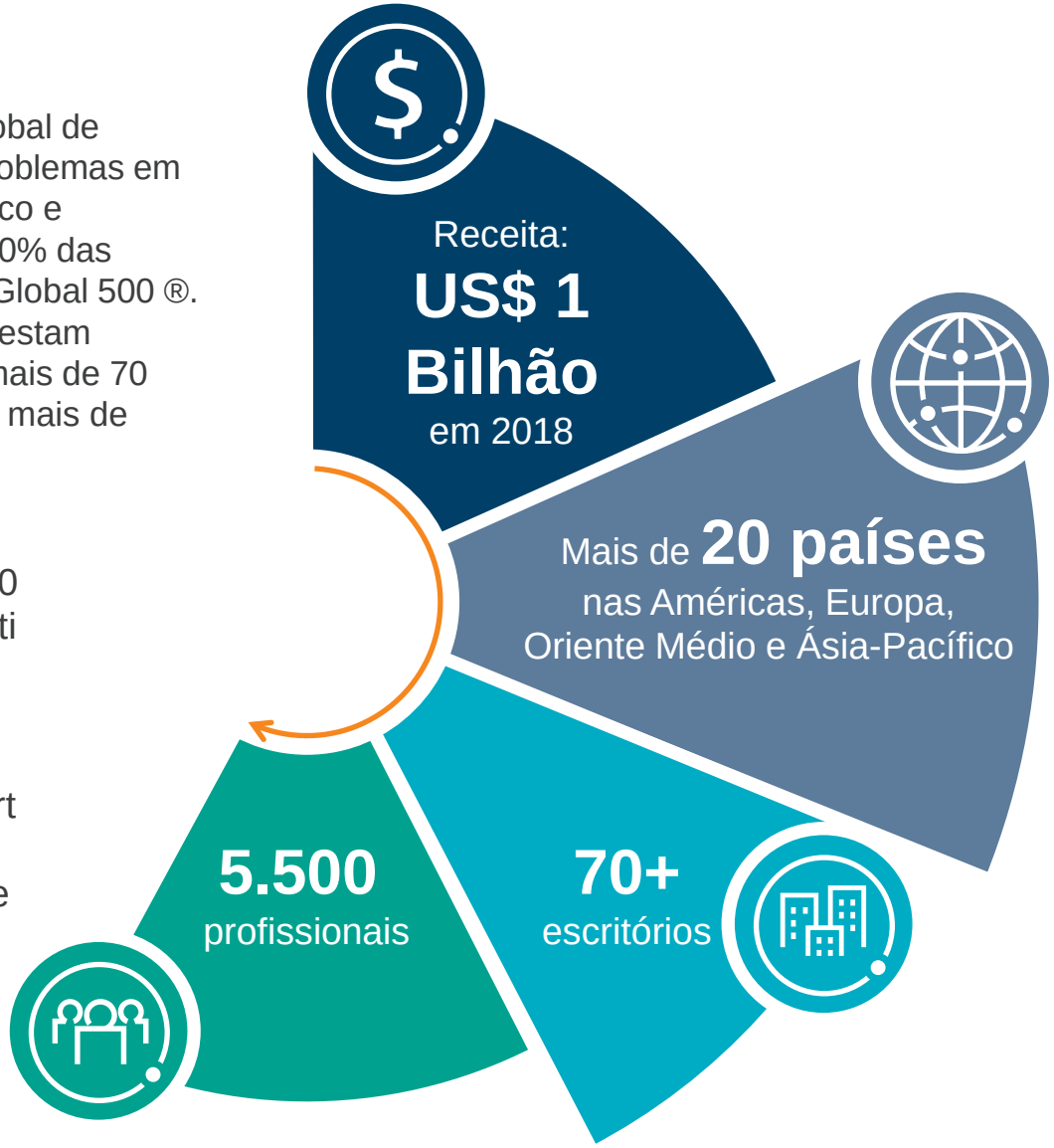
ABORDAGEM PARA ADEQUAÇÃO À LGPD

Internal Audit, Risk, Business & Technology Consulting

A PROTIVITI

A Protiviti (www.protiviti.com) é uma empresa global de consultoria que ajuda empresas a resolverem problemas em finanças, tecnologia, operações, governança, risco e auditoria interna. Presta serviços para mais de 60% das empresas da Fortune 1000® e 35% da Fortune Global 500 ®. Protiviti e suas firmas membro independentes prestam serviços aos clientes por meio de uma rede de mais de 70 escritórios em mais de 20 países, contando com mais de 4.000 profissionais em todo o mundo *.

Classificação 57 na lista de 2016 Fortune 100 Melhores Empresas para Trabalhar®, Protiviti frequentemente recebe elogios e é reconhecida em seu segmento entre as “Melhores Empresas para Trabalhar". A empresa é uma subsidiária integral da Robert Half (NYSE: RHI). Fundada em 1948, a Robert Half é membro do índice S & P 500, e foi nomeada para Fortune® lista "Empresas Mais Admiradas do Mundo" da revista 1998-2016.



***A ICTS é a *firma membro* da Protiviti no Brasil.**

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti

CENÁRIO REGULATÓRIO E LGPD

CONTEXTO: CENÁRIO REGULATÓRIO

Brasil

a Lei Geral de Proteção de Dados pessoais - lei da Câmara 13.709/18. A lei disciplina a forma como informações são coletadas e tratadas, especialmente em meios digitais, como dados pessoais de cadastro ou até mesmo textos e fotos publicados em redes sociais. Caso seja constatada alguma irregularidade, a empresa pode receber uma série de sanções, entre as quais está prevista a ***multa diária de até 2% do faturamento, com limite de R$ 50 milhões****. As empresas devem se adequar até* ***Agosto de 2020****.*

União Européia

O regulamento geral de proteção de dados imporia uma legislação robusta e harmonizada em matéria de proteção de dados em toda a UE.

Asia

Cingapura, Malásia, Filipinas, Coréia do Sul e Taiwan introduziram, nos últimos cinco anos, regimes abrangentes de proteção de dados em suas respectivas jurisdições.

Estados Unidos

Nos últimos anos, o governo federal implementou uma supervisão mais rígida e promulgou requisitos específicos de gerenciamento e divulgação de riscos cibernéticos para os setores de saúde, defesa, energia e outros setores da indústria de infraestrutura crítica.

Africa do Sul

A Lei de Proteção de Informações Pessoais (Popi) da África do Sul, que entrou em vigor em novembro de 2013, regula como qualquer pessoa que processa informações pessoais deve manipular, manter e proteger essas informações.

Australia

A Lei de Privacidade (Enhancing Privacy Protection) de 2012 foi introduzida como uma emenda à Privacy Act 1988, uma lei australiana que regula o manuseio de informações pessoais sobre indivíduos.

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

- Qualquer empresa ou órgão público deve ser **responsabiliza-do em caso de violação à lei**

- Conceitua **dado pessoal, dado sensível e dado pseudonimizados e dado anonimizado.**

- Cobra que órgãos públicos organizem dados de forma "**interoperáveis**" e "**estruturados**

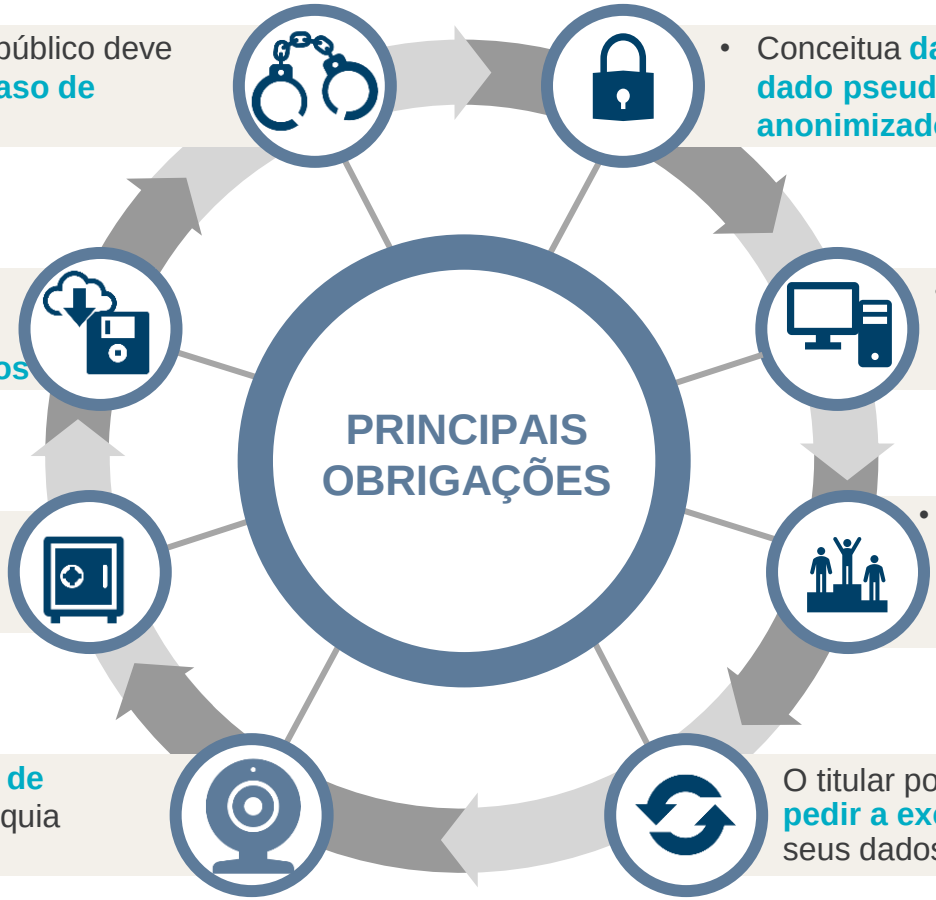
- Todo tratamento de dados pessoais feito no Brasil **em "meios digitais" ou fora dele**

- Multa diária de **até 2% do faturamento**, com limite de R$ 50 milhões

- Uma empresa ou órgão público só poderá fazê-lo se tiver o **consentimento do titular** dos dados

- Cria-se a **Autoridade Nacional de Proteção de Dados**, uma autarquia vinculada à Presidência

O titular pode retirar seu **consentimento, pedir a exclusão ou a portabilidade** dos seus dados pessoais.



© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti

QUAIS DADOS CONSIDERAR

IDENTIFICADORES

- Nome
- Endereço
- Email
- Passporte
- Info financeira & bancária
- Data de nascimento
- Dados de saúde
- Dados biométricos
- ID do funcionário
- Número de telefone

IDENTIFICADORES ONLINE

- Endereços IP, estáticos e dinâmicos
- Endereços MAC
- Cookies (WWW)
- IDs de equipamento móvel internacional (IMEI)
- Identidade de assinante móvel internacional (IMSI)
- Unique mobile device identifiers (UDID)
- IDs de publicidade
- GPS ou outros dados de localização
- Arquivos de log
- Browser fingerprints

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

UM PROGRAMA EFICAZ

NECESSIDADES CONTÍNUAS DE COMPLIANCE

O principal objetivo do Programa de Privacidade & Proteção de dados é manter o tratamento das informações pessoais de maneira legal, justa, segura e confidencial enquanto permite que os indivíduos exerçam os seus direitos de privacidade. O ciclo das necessidades contínuas de compliance representado abaixo ajuda as organizações na implementação e manutenção das boas práticas de privacidade e proteção de dados para se manter em conformidade com a LGPD e demais regulações sobre privacidade

Monitoramento

- Estamos em conformidade com a LGPD?
- Podemos comprovar essa conformidade?
- Como sabemos se o nosso programa é bem sucedido?
- Há envolvimento dos times de auditoria?
- Há reporte para o Board e os Executivos?
- Estamos sendo auditados por ou reportamos algo a órgãos reguladores (ANPD)?

Identificação

- Sabemos quais os dados que temos?
- Sabemos onde os dados estão localizados?
- Sabemos como os dados estão sendo usados?
- Por onde esses dados transitam?

Execução

- Sabemos quem é responsável pelos assuntos?
- As áreas de negócio entendem quais são suas obrigações?
- A área de TI entende quais são suas obrigações?
- As responsabilidades foram formalmente aceitas?
- Como a área Jurídica e de TI interagem com o Encarregado e o seu time?

Avaliação

- Classificamos os nossos dados?
- Avaliamos o risco de privacidade de nossas operações?
- Avaliamos o risco de proteção de dados de nossas operações?
- Estamos envolvidos em atividades de processamento de alto risco que podem exigir controles adicionais?

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

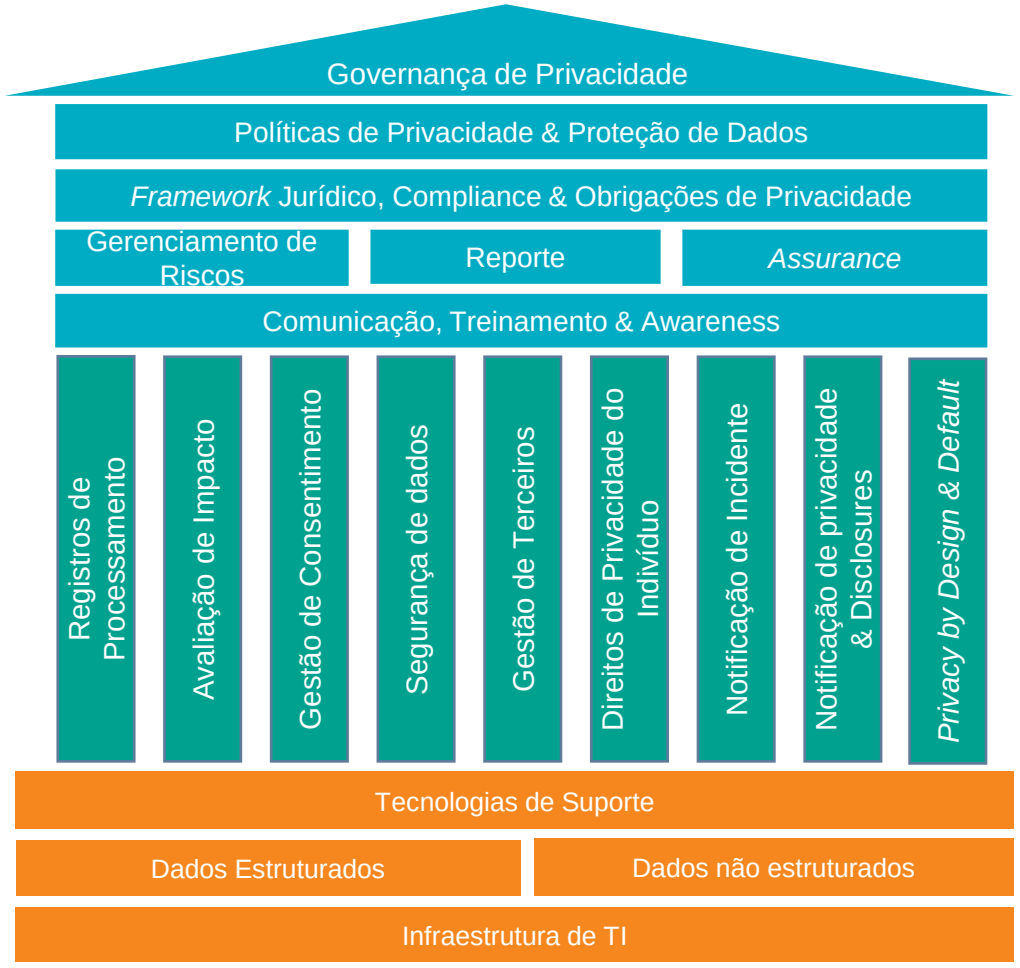
protiviti

PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS

Definir o Programa e Governança

Implantar Controles Operacionais

Definir budget e apoiar soluções tecnológicas

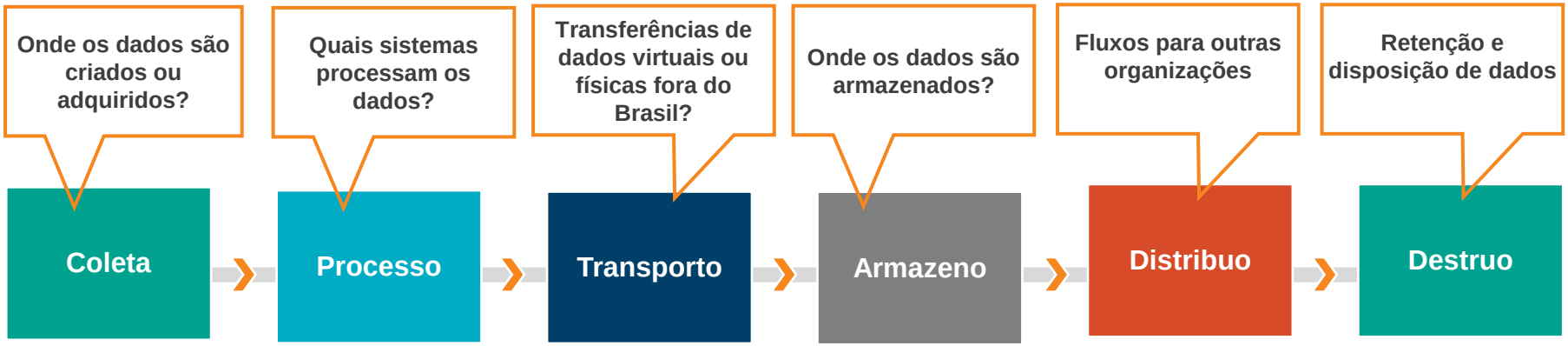


© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti

ONDE COMEÇAR

Cadastro de dados – aplicações e terceiros



As aplicações e os terceiros devem ser priorizados:
Alto risco – alta probabilidade de que uma violação de dados pode ocorrer
Risco médio – probabilidade moderada de que uma violação de dados pode ocorrer
Baixo risco – baixa probabilidade de que uma violação de dados pode ocorrer

IMPACTOS LEGAIS | **IMPACTOS ORGANIZACIONAIS** | **IMPACTOS DE TI**

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
protiviti

LIÇÕES APRENDIDAS

COMECE COM UMA AVALIAÇÃO DE IMPACTO SOBRE PRIVACIDADE DE DADOS

Um DPIA deve conter pelo menos:

- Uma descrição geral das operações de tratamento previstas.
- Uma avaliação dos riscos para os direitos e liberdades dos titulares de dados.
- As medidas previstas para abordar esses riscos, salvaguardas, medidas de segurança e mecanismos para garantir a protecção dos dados pessoais.

IDENTIFIQUE QUE TIPO E VOLUME DE DADOS PRIVADOS VOCÊ USA

- Informações pessoais
- Informações confidenciais
- Dados de funcionários e clientes
-

IDENTIFIQUE ONDE VOCÊ USA/COMPARTILHA DE ONDE VEIO

- CRM, sistemas de RH, Web sites de clientes
- Fontes de dados de terceiros
- Fornecedores de terceiros – marketing, comunicações, análises, relatórios
- Processos – consentimento, embarque, embarque, qualidade dos dados, manuseio de reclamações, notificação

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti

LIÇÕES APRENDIDAS

CONSIDERAÇÕES-CHAVE

- Criar uma sensação de urgência
- LGPD não é uma responsabilidade de um departamento: exigirá colaboração ampla da empresa
- Foco nos principais riscos de privacidade (dados altamente sensíveis mantidos em massa; dados do consumidor; dados utilizados de forma a que o titular dos dados possa não estar consciente ou consentido; processos de gestão de privacidade).
- Comece de cima para baixo, olhando para as operações de negócios/fluxos de receita vs bottom up controles/políticas.
- A LGPD não é um programa de segurança da informação.
- Escolha o oficial de proteção de dados correto ("DPO").
- Entrar no início – a privacidade pode causar interrupções na transformação digital.
- Esclareça suas responsabilidades como Controlador e Processador.
- Não se esqueça de suas terceiras partes.
- A manutenção da evidência de Compliance é fundamental.

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti

Face the Future with Confidence

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti®